

REMARKS

The above amendments to the claims were originally submitted in a preliminary amendment mailed October 11, 2005. But, it is believed that the preliminary amendment and the current office action crossed in the mails and that this preliminary amendment has not been entered. Therefore, the claim amendments are being resubmitted.

Please cancel claims 1-23 (including two claims both numbered "22", for total of twenty four claims canceled). New claims 25-38 have been added (the first new claim beginning with the next available claim number). Claims 25-38 are now pending in this application.

The Prior Art Problem to be Solved

New claim 25 is a method for assessing the risk of fraud of a financial transaction within a distributed system, and new claim 32 claims a distributed risk assessment system for assessing the risk of fraud of a financial transaction.

Prior art fraud detection systems detect fraud by processing transactional data at a central server. Unfortunately, additional data located at the precise source of the transaction is not transmitted to the central server for processing, and thus a complete risk assessment cannot be performed. In other words, performing risk scoring at a single, central location generally does not enable all of the available detail regarding that transaction to be included in the risk assessment.

For example, if a central scoring location receives transactional data indicating a \$5,000 purchase of computer equipment, there is no additional data received indicating whether a single item was purchased or whether five \$1,000 computers were purchased (even though the purchase of five computers would be considered riskier). This problem is especially prevalent in online transactions. Other examples of at-source data that are typically not sent to a central location to be included in a risk assessment include Web browser information, a TCP/IP address, an e-mail address, server information, etc. The problem to be solved then, is how to include this remote, at source data, in the assessment of risk of a financial transaction.

One solution might be to make a concerted effort to send ALL at-source data from remote locations to a central server for processing. But, this approach is problematic in that it can be difficult to arrange for all the data to be transmitted centrally, the types of data can change thus requiring the central server to adapt to new data fields, and data privacy issues emerge when sensitive information is being sent to a central site.

The Present Invention

Even though technical hurdles exist, the best way to solve this problem is to perform processing and scoring of the transactional data both centrally and on local client computers. But because additional at-source information (that might be sensitive) is now being used at distributed locations to assess risk (and because certain information will be sent from a central location to a distributed location), the data is encrypted and processing is performed on the encrypted data, thus eliminating the possibility of releasing sensitive information. It is further realized that because the data is being processed both centrally and at distributed client locations, that novel techniques for processing the data can be used. It is through a combination of these techniques that the presently claimed invention addresses the above problem.

For example, claim 25 requires that first and second financial transactions are received at a central computer system. These transactions represent a financial transaction for a particular account and a previous transaction for that account. Features are generated for each transaction and the changes between these features are then determined at the central server. As is known to one of skill in the art, use of *features* (or *characteristic variables*) is a known technique of assessing risk based upon sets of data. Before these feature changes are transmitted to a client computer system for further processing claim 25 requires that they are encrypted to prevent the release of any sensitive information.

The Cited Art Distinguished

As explained above and as required by claim 25 (for example), the present invention relates to assessing financial fraud risk within a distributed system and uses analyses of financial transactions and features generated from those transactions to help assess the risk. The cited reference, *Shambroom*, has nothing to do with assessing the risk of a financial transaction. By contrast, *Shambroom* deals with improving the security of messages transmitted from a client

through a network server to a destination server (Abstract, column 1). *Shambroom* does not disclose financial transactions, does not disclose generating features from financial transactions, does not disclose encrypting feature changes, and does not disclose scoring a result to produce a fraud risk value. For least these reasons, *Shambroom* is not applicable as a reference to the presently claimed invention.

Shambroom might be relevant only in the sense that it does disclose a distributed computing system. Also, the original claims did require "keys" (a data structure used to group information about a transaction) and *Shambroom* does disclose use of cryptographic keys, but these two types of keys are different, and in any case, the currently pending claims do not require "keys."

The cited reference *Basch* does disclose predicting financial risk and analysis of financial transactions, but does not disclose the novel techniques claimed such as assessing risk over a distributed system and the generation of features from encryption transactions.

Claim Rejections

Original claim 8 had been rejected in that the step of "receiving information . . ." did not specify which entity is receiving the information. Claim 8 has been canceled, although Applicant points out that new claim 25 requires a first step in which first and second financial transactions are specifically received at a central computer system. Claim 8 was also rejected in that the claim did not specify which entity generates a first set of keys. New claim 25

specifically requires that first features for a financial transaction are generated at the central computer system. Applicant submits that the remaining steps of new claim 25 do specify where each step is occurring in contrast with the other steps of original claim 8 that the Examiner had rejected.

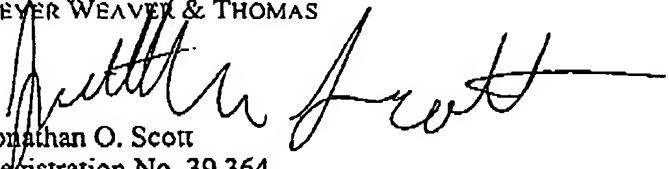
Claims 2 and 17 had been rejected but have since been canceled.

Claim Objections

The Examiner's objections to the numbering of the original claims has been taken into account and the new claims have been renumbered to start with the next available claim number, namely, "25."

Consideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS


Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
Telephone: (612) 252-3330
Facsimile: (612) 825-6304